



NATURAL

Natural SAF Security

Version 3.1.6

 **SOFTWARE AG**



This document applies to Natural SAF Security Version 3.1.6 and to all subsequent releases. Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

© June 2002, Software AG
All rights reserved

Software AG and/or all Software AG products are either trademarks or registered trademarks of Software AG. Other products and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents






Natural SAF Security - Overview	1
Natural SAF Security - Overview	1
Introducing Natural SAF Security	2
Introducing Natural SAF Security	2
What is Natural SAF Security?	2
Natural Security Related Considerations	3
Automatic Logon	3
PROFILE Command	3
Library SYSSEC	3
Transition Period Logon	3
Utilities	3
Installing Natural SAF Security	4
Installing Natural SAF Security	4
Prerequisites	4
Tape Contents	4
Installation Procedure	4
Step 1: Load Modules and Error Messages	4
Step 2: Adjust Natural Parameter Module	5
Step 3: Relink Natural	5
Step 4: Install the SAF Server	5
Step 5: Activate Natural SAF Security	6
Defining Resources in the External Security System	7
Defining Resources in the External Security System	7
Users	7
Environments	7
Libraries	8
Environment-Independent Access to a Library	8
Access to a Library in Specific Environments	8
Use of System Commands in a Library	8
Modifications on FUSER System File	9
Translation and Effects of Access Levels	9
RPC Services	9
Environment-Independent Use of an RPC Service	9
Use of an RPC Service in Specific Environments	10
User-Defined Resources	10
Environment-Independent Use of a User-Defined Resource	10
Use of a User-Defined Resource in Specific Environments	10
Overview of Resource-Class Definitions	11
Administrator Services	12
Administrator Services	12
General NSF Options	12
General NSF Options - Screen 1	12
Security System	12
User Options	13
General NSF Options - Screen 2	14
Environment Options	14
Library Options	15
RPC Options	16
User-Resource Options	17
Definition of System-File Environments	17
Define System-File Environments Screen	17
Available Functions	17
Components of an Environment Profile	18

NSF Online Services	19
System Parameters	19
System Statistics	20
User Statistics	21
Zap Maintenance	21
Storage Display	21
System Tracing	21
Server Restart	21
User Exits	22
User Exits	22
Overview of User Exits	22
User Exits for User and Password Authentication	22
NSFNPAS	22
NSFNPASZ	23
NSFNPAX	23
User Exit for Checking Resource Access to Dedicated API Class	24
User Exit for Maintaining Resource Profiles	24
User Exits for Checking Access Rights to a Resource	25
User Exit for Obtaining Information from the SAF Server	25

Natural SAF Security - Overview

This documentation describes all functions of Natural SAF Security. It covers the topics listed below.

The reader is assumed to be familiar with and have a good general understanding of Natural and Natural Security. In particular the reader is assumed to be familiar with the Natural Security documentation.

- | | |
|--|--|
|  Introducing Natural SAF Security | Basic concepts of Natural SAF Security. |
|  Installing Natural SAF Security | How to install Natural SAF Security. |
|  Defining Resources in the External Security System | Considerations concerning the external security system used with Natural SAF Security. |
|  Administrator Services | Natural SAF Security administration functions in Natural Security. |
|  User Exits | Information on the available user exits. |

Natural SAF Security uses a SAF server, which is described in the SAF Security Kernel documentation.

For information on changes, enhancements and new features provided with this version, see the Natural Release Notes.

Introducing Natural SAF Security

This section provides an overview of Natural SAF Security. It covers the following topics:

- What is Natural SAF Security?
 - Natural Security Related Considerations
-

What is Natural SAF Security?

Natural SAF Security is an add-on product to Natural Security. It allows you to protect your Natural applications and control the access to Natural sessions using resources defined in an external security system. With Natural SAF Security, you can protect your Natural sessions by combining security definitions made in Natural Security and in the external security system.

This external security system must be an SAF-compliant security system. At present, Natural SAF Security supports the following external security systems:

- RACF,
- CA-ACF2,
- CA Top Secret.

With Natural SAF Security, it is no longer necessary to define security profiles for individual users in Natural Security. Instead, existing user definitions made in the external security system can be used.

When you use Natural SAF Security, you need not define users both in Natural Security and in an external security system; it is sufficient to define them in the external security system. You only need to define user **groups** in Natural Security. When Natural SAF Security is active and a user logs on to Natural, the user authorization checks will be done using the user ID and user password from the external security system.

The group ID from the external security system is passed to Natural Security, and will be used for further security checks, particularly concerning the use of Natural libraries and utilities. Although library protection via an external security system is possible, the Natural Security library security profiles provide more sophisticated and more adequate mechanisms for protecting Natural libraries.

In addition, the protection of Natural can be made environment-specific. A Natural environment is determined by the combination of the system files FNAT, FUSER, FSEC and FDIC. You can define a profile for each system-file combination and control users' access to it. Thus it is possible to fully separate the protection of a Natural development environment from that of a Natural production environment.

Moreover, Natural SAF Security allows you to protect user-defined resources which are defined in the external security system against unauthorized use.

Natural SAF Security also provides Natural RPC protection: With Natural Security, certain RPC options can be set in library profiles, thus making the use of Natural RPC functions dependent on the library from which they are invoked. Natural SAF Security, on the other hand, allows you to protect Natural RPC services (that is, Natural subprograms invoked remote via Natural RPC) as such against unauthorized use.

The generation of end of transaction IDs (ETIDs) can also be controlled via Natural SAF Security.

Natural Security Related Considerations

The following Natural Security items should be considered when using Natural SAF Security.

Automatic Logon

If the Natural profile parameter AUTO=ON (Automatic Logon) is set, a user can only log on to Natural if a default library is defined for him/her. The default library can be defined either in the Natural Security group security profile or in the external security system. See also the section Automatic Logon in the Natural Security documentation.

PROFILE Command

When Natural SAF Security is active, the Natural system command PROFILE indicates whether the user and his/her group are defined in Natural Security:

- If neither the current user ID nor group ID are defined in Natural Security, the user type will be shown as "Ext. User".
- If the current user ID is not defined in Natural Security, but the current group ID is defined in Natural Security, the user type will be shown as "Ext. User/Grp".

Library SYSSEC

The library SYSSEC can only be accessed by users who are defined as "Administrators" in Natural Security.

Transition Period Logon

If the Natural Security general option Transition Period Logon is set to "N", only unprotected libraries can be accessed via Natural SAF Security. Undefined libraries can only be accessed if Transition Period Logon is set to "Y".

Utilities

For users for whom neither a user security profile nor a group security profile exists in Natural Security, the default utility profiles apply.

For users for whom no user security profile, but a group security profile exists, the use of utilities is controlled by the group-library-specific utility profiles and group-specific utility profiles associated with this group.

Installing Natural SAF Security

This section describes how to install Natural SAF Security. It covers the following topics:

- Prerequisites
 - Tape Contents
 - Installation Procedure
-

Prerequisites

Natural SAF Security can only be installed if the following products have been installed:

- Natural Version 3.1.6 (or above),
- Natural Security Version 3.1.6 (or above),
- Adabas (or Adabas Limited library) Version 6.2 (or above),
- the SAF server,
- an SAF-compliant security system.

Tape Contents

The Natural SAF Security installation tape contains the following datasets (*nnn* in the dataset names denoting the version number):

Dataset	Contents
NSFnnn.ALLINPL	The Natural INPL dataset containing updates to Natural Security.
NSFnnn.ALLERRN	Natural error messages.
NSFnnn.MVSSRCE	The source library, containing Assembler source books, macros and examples.
NSFnnn.MVSLOAD	The load library, containing the Natural SAF Security assembly module NATGWSAF.
NSFnnn.MVSJOBS	Example jobs for installing Natural SAF Security.

Installation Procedure

This section describes step by step how to install Natural SAF Security.

Step 1: Load Modules and Error Messages

(Job I005)

Note:

The INPL job will overwrite the Natural Security user exit LOGONEX1. If you have modified this user exit, please take care to secure your modified copy appropriately (by copying it into one of your own libraries) before you execute this job.

Load the Natural SAF Security modules and error messages using the Natural utility INPL (assigning NSFnnn.ALLINPL to CMWKF01) and the SYSERR utility program ERRLODUS (assigning NSFnnn.ALLERRN to CMWKF02) respectively.

Step 2: Adjust Natural Parameter Module

(Job I010)

Add the following parameters to your Natural parameter modules:

```
IDSIZE=8
RDCSIZE=4
```

Then reassemble the parameter modules.

Step 3: Relink Natural

(Job I060 from the Natural installation tape)

Relink your Natural nucleus to include the modified parameter module and Natural SAF Security modules:

```
INCLUDE SMALOAD (NATPARM)
INCLUDE NSFLOAD (NATGWSAF)
```

Step 4: Install the SAF Server

Install the SAF server as described in the SAF Security Kernel documentation.

In the configuration module of the SAF server, the following Natural SAF Security options may have to be set:

Number of Cached Resource Checks

Natural SAF Security allows you to have resource checks cached. If you wish resource checks to be cached, you have to specify the number of successful resource checks to be cached for each resource class, using the following parameters of the configuration module:

Parameter	Default Value	Function
NANUSF	0	Number of cached environment checks.
NANUTC	0	Number of cached library checks.
NANUSV	0	Number of cached RPC-service checks.

Alternate Resource Names

If you wish to change the default names for the resource classes, you have to change the following parameters of the configuration module:

Parameter	Default Value	Function
NACLSF	NSFSAG	Resource-class name for environments.
NACLTC	NTCSAG	Resource-class name for libraries.
NACLSV	NSVSAG	Resource-class name for RPC services.
NACLAP	NPGSAG	Resource-class name for user-defined resources.

Natural SAF Security Options

The following parameters need not be set in the configuration module; the corresponding options are defined in the General NSF Options.

Parameter	Option
NAXTPG	User Options: NSF *GROUP
NAXTNM	User Options: NSF *USER-NAME
NAGENET	User Options: NSF *ETID
NACKSF	Environment Options: Protect Environments
NAUNSF	Environment Options: Allow Undefined Environments
NACKTC	Library Options: Protect Libraries
NAENVTC	Library Options: with Environment
NACMDL	Library Options: Disable Natural Commands
NAPOBJ	Library Options: Set FUSER Read-Only
NACKSV	RPC Options: Protect Services
NAENVSV	RPC Options: with Environment
NACKPG	User-Resource Options: with Environment
NAUNAP	User-Resource Options: Allow Undefined Resources

Note:

Any configuration-module parameters whose names begin with "NA" and which are *not* listed in the three tables above, need not be specified. They will not be evaluated by Natural SAF Security.

Step 5: Activate Natural SAF Security

To perform this step, the following prerequisites must be met in Natural Security: You have to be defined as a user of type "Administrator", and you have to be linked to the library SYSSEC.

To activate Natural SAF Security:

1. Invoke Natural and log on to the Natural Security library SYSSEC.
2. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed.
3. Select "Set general options". The Set General Options screen will be displayed.
4. Press PF8 (NSF1). The General NSF Options screen will be displayed.
5. Set all four options listed under "Security System" on this screen.

The setting of these options activates Natural SAF Security with default settings. Once the SAF server has been configured appropriately and has been started, access to Natural is now controlled by Natural SAF Security.

Note:

Before you change any default settings, make sure that the corresponding resources are defined in the external security system being used. For resource definitions, see the section Defining Resources in the External Security System.

The load job performed in Step 1 loads the new utility library SYSNSFOS. This library contains the NSF Online Services (it corresponds to the library SYSSAF supplied with Entire Security SAF Security). To be able to access this utility, a utility security profile has to be defined for it in Natural Security.

Defining Resources in the External Security System

This section describes which resources have to be defined in the external security system in conjunction with Natural SAF Security. It covers the following topics:

- Users
- Environments
- Libraries
- RPC Services
- User-Defined Resources
- Overview of Resource-Class Definitions

Note:

Some external security systems use the term "resource profile", others the term "rule". In this documentation the term "resource profile" is used.

Some external security systems use the term "resource class", others the term "resource type". In this documentation the term "resource class" is used.

Users

No special user-specific definitions have to be made in the external security system.

If the General NSF Options "NSF *GROUP" and "NSF *USER-NAME" are set to "Y", the user's group and user name as defined in the external security system are passed to Natural SAF Security.

Environments

With Natural SAF Security, Natural environments can be protected to prevent unauthorized users from accessing the system files.

A Natural environment is determined by the combination of the Natural system files FNAT, FDIC, FSEC and FUSER. For each system-file combination that is to be protected, a resource profile has to be defined in the external security system. The identification of the resource profile must be a 40-digit number corresponding to the database ID / file number (DBID/FNR) combinations of the four system files. The database IDs and file numbers must be specified in the following sequence:

1) FNAT DBID, 2) FNAT FNR, 3) FDIC DBID, 4) FDIC FNR, 5) FSEC DBID, 6) FSEC FNR, 7) FUSER DBID, 8) FUSER FNR.

Each DBID and FNR must be specified as a 5-digit number (padded with leading zeros).

Example:

```
0001100035000110003300011000340001100032
```

The above specification would refer to the following environment:

```
FNAT=(00011,00035), FDIC=(00011,00033), FSEC=(00011,00034), FUSER=(00011,00032)
```

The option "Protect Environments" in the General NSF Options determines if access to a Natural environment is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for the environment in the external security system determines whether a user has access to it or not. A user needs at least READ access to be able to access a Natural environment.

The resource-class name for Natural environments is defined with the macro parameter NACLSF in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSFSAG".

Libraries

With Natural SAF Security, Natural libraries can be protected to control users' access to them.

You can protect a Natural library:

- independently of the environment, or
- in specific environments.

The resource-class name for Natural libraries is defined with the macro parameter NACLTC in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NTCSAG".

Environment-Independent Access to a Library

If a Natural library is to be protected, a resource profile has to be defined for it in the external security system.

The resource-profile name must correspond to the library ID and may be up to 8 characters long.

The option "Protect Libraries" in the General NSF Options determines if access to Natural libraries is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for a library in the external security system determines whether a user can log on to the library or not. The access level is checked when a users logs on to a Natural library. A user needs at least READ access to be able to log on to a library.

Access to a Library in Specific Environments

If a Natural library is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-library combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias and the library ID (up to 8 characters), separated by a period:

a.library-ID

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific library-access check is activated by the option "with Environment" in the Library Options section of the General NSF Options. Access to the library is then only possible in environments to which the user has READ access.

Use of System Commands in a Library

If the option "Disable Natural Commands" in the General NSF Options is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not users may use Natural system commands within the library. If the option is set to "Y", users need at least CONTROL access to use system commands.

Modifications on FUSER System File

If the option "Set FUSER Read-Only" in the General NSF Options is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not the user may make modifications on the FUSER system file from within the library. If the option is set to "Y", users need at least ALTER access to make modifications on the FUSER file.

Translation and Effects of Access Levels

The following table shows how CA-ACF2 translates RACF attributes, and also gives an overview of the effects of the access levels:

RACF Attribute	CA-ACF2 Resource Rule	Disabling of Natural Commands	Read-Only FUSER System File
READ	READ	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
UPDATE	UPDATE	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
CONTROL	DELETE	Commands are allowed (same as profile parameter NC=OFF).	FUSER file is read-only.
ALTER	ADD	Commands are allowed (same as profile parameter NC=OFF).	Modification on FUSER file are allowed.

RPC Services

With Natural SAF Security, Natural RPC services can be protected against unauthorized use.

You can protect a Natural RPC service:

- independently of the environment, or
- in specific environments.

The resource-class name for Natural RPC services is defined with the macro parameter NACLSV in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSVSAG".

Environment-Independent Use of an RPC Service

If a Natural RPC service is to be protected, a resource profile has to be defined for it in the external security system.

The resource-profile name must correspond to the library ID and subprogram name, each of which may be up to 8 characters long and which must be separated by a period:

library-ID.subprogram-name

The option "Protect Services" in the General NSF Options determines if access to Natural RPC services is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for the RPC service in the external security system determines whether a user can use the service or not. A user needs at least READ access to be able to execute a Natural subprogram via RPC.

Use of an RPC Service in Specific Environments

If a Natural RPC service is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-service combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias, the library ID (up to 8 characters), and the subprogram name, separated from one another by periods:

a.library-ID.subprogram-name

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific service-access check is activated by the option "with Environment" in the RPC Options section of the General NSF Options. Use of the RPC service is then only possible in environments to which the user has READ access.

User-Defined Resources

With Natural SAF Security, user-defined resources can be protected against unauthorized use.

You can protect a user-defined resource:

- independently of the environment, or
- in specific environments.

The resource-class name for user-defined resources is defined with the macro parameter NACLAP in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NPGSAG".

Environment-Independent Use of a User-Defined Resource

If a user-defined resource is to be protected, a resource profile has to be defined for it in the external security system.

The name of a resource profile can, for example, consist of a library ID, main function and subfunction. The library ID may be up to 8 characters long, the main function is usually (but not necessarily) the name of the programming object, and the subfunction is a 3-character code identifying the function to be performed. Each of the three must be separated from one another by a period:

library-ID.main-function.sub-function

The resource profile determines whether a user may access a user-defined resource or not.

The necessary security requests are handled via user exits provided by Natural SAF Security. The user exits are described in the section User Exits.

Use of a User-Defined Resource in Specific Environments

If a user-defined resource is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-resource combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name is composed as above,

prefixed by the alias, for example:

a.library-ID.main-function.sub-function

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific resource-access check is activated by the option "with Environment" in the User-Resource Options section of the General NSF Options.

The necessary security requests are handled via user exits provided by Natural SAF Security. The user exits are described in the section User Exits.

Overview of Resource-Class Definitions

The following table summarizes the resource-class definitions to be made in the configuration module of the SAF server:

Resource	Macro Parameter in Configuration Module	Default Name	Length of Resource-Profile Name
Environments	NACLSF	NSFSAG	40
Libraries	NACLTC	NTCSAG	10
RPC services	NACLSV	NSVSAG	19
User-defined resources	NACLAP	NPGSAG	23

Administrator Services

If Natural SAF Security is installed, the Administrator Services subsystem of Natural Security provides the following additional functions, which are used in conjunction with Natural SAF Security:

- General NSF Options
- Definition of System-File Environments
- NSF Online Services

In order to perform these Natural SAF Security functions, you need to have access to the Natural Security library SYSSEC. Also, you have to be defined in Natural Security as a user of type "Administrator". Moreover, you need to have access the Administrator Services subsystem of Natural Security (as described in the section Access to Administrator Services of the Natural Security documentation).

Note:

Be careful when using the user ID "DBA": If you log on to SYSSEC as user "DBA", any Natural SAF Security settings and checks will be ignored. As indicated in the Natural Security installation documentation, the user ID "DBA" should only be used for the initial definition of Natural Security administrators and for recovering the Natural Security environment.

General NSF Options

This function is used to set various Natural SAF Security options.

For any changes of these options to take effect, you have to restart your Natural session.

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 1, select "Set general options". The Set General Options screen will be displayed.
3. Press PF8 (NSF1). The General NSF Options screen will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.

General NSF Options - Screen 1

On the first General NSF Options screen, you can set the following options:

Security System

Option	Explanation
External Security System	<p>In this field, you specify the external security system to be used.</p> <p>Possible values are: RACF, ACF2 (= CA-ACF2) and TOPS (= CA Top Secret) and SAF.</p> <p>The default value is "SAF": this means that only General NSF Options which apply to all supported external security systems are evaluated, while those which are specific to a certain security system will be ignored.</p> <p>Note: The value of this option is evaluated internally by Natural SAF Security only, but is not communicated to the SAF server. In the SAF server, the external security system is specified in the configuration module.</p>
Server ID	In this field, you specify the node ID of the SAF server to be used (that is, the value of the parameter GWDBID as specified in the SAF server installation).
Natural Security	<i>This field is reserved for future use. At present, it must contain "FSEC".</i>
Protection Level	<p>This field is used to activate Natural SAF Security. Possible values are:</p> <p>1 - Natural SAF Security security is not active, and the SAF server is not accessed. Access to the Natural session is controlled by Natural Security.</p> <p>2 - Natural SAF Security security is active. Access to the Natural session is controlled by the SAF server. <i>Within</i> the session, Natural Security determines what users are allowed to do.</p>

User Options

Option	Explanation
NSF *GROUP	<p>Determines whether the group ID defined in the external security system is to be used as value for the Natural system variable *GROUP (Y/N).</p> <p>It is recommended that this option be set to "Y" (see also option "NSC Group ID" below).</p>
NSC Group ID	<p>Determines whether the group IDs defined in the external security system also have to be defined in Natural Security (Y/N).</p> <p>It is recommended that this option be set to "Y"; any conditions of use associated with the Natural Security group profile can then be controlled by Natural Security.</p>
NSF *USER-NAME	Determines whether the user name defined in the external security system is to be used as value for the Natural system variable *USER-NAME (Y/N).
NSC User ID	<p>Determines whether, in addition to being defined in the external security system, users also have to be defined in Natural Security (Y/N).</p> <p>If set to "Y", the Natural Security user profile will be used once the user has successfully logged on to the external security system. After the initial logon, the conditions of use associated with the Natural Security user profile will be controlled by Natural Security. However, Natural Security will not perform any password checks.</p>
NSF *ETID	<p>Determines if and how ETIDs (end of transaction IDs) are to be generated by Natural SAF Security at the start of the Natural session:</p> <p>N No ETIDs are generated by Natural SAF Security; they are generated by Natural Security.</p> <p>O Generate ETIDs only for online users.</p> <p>B Generate ETIDs only for batch-mode users.</p> <p>A Generate ETIDs for all (online and batch-mode) users.</p> <p>J Use the job name as ETID (for batch-mode users only).</p> <p>T Use the value of the Natural system variable *INIT-ID as ETID.</p>
NSC Logon Priv. Library	Determines whether users are to be able to access other users' private libraries (provided the external security system allows this) (Y/N).

General NSF Options - Screen 2

On the second General NSF Options screen, you can set the following options:

Environment Options

Option	Explanation
Protect Environments	<p>Determines whether the environment profile of the system-file combination (FNAT, FUSER, FDIC, FSEC) is to be checked at the logon (Y/N).</p> <ul style="list-style-type: none">• If this is set to "Y", the access level defined for the environment in the external security system determines whether a user has access to it or not.• If this is set to "N", users have access to any environment. <p>See also Definition of System-File Environments below.</p>
Allow Undef. Environments	<p>Determines whether undefined system-file combinations are to be accepted at the logon (Y/N).</p> <p>This option is only relevant if RACF is used as external security system. With other external security systems, this option will be ignored.</p>

Library Options

Option	Explanation
Protect Libraries	<p>Determines whether the library access level is to be checked via the SAF server (Y/N/R).</p> <ul style="list-style-type: none"> • Y - Users need at least READ access to log on to a library. • N - Access to libraries is controlled by Natural Security according to the Natural Security logon rules. • R - If RACF is used as external security system, you can set this option to "R": The library access level will be checked, but access to libraries not defined in RACF will also be possible. For other security systems, "R" is not possible.
with Environment	<p>Determines whether the environment alias is to be used as prefix of the resource library for the access-level check (Y/N).</p> <p>See also Definition of System-File Environments below.</p>
Disable Natural Commands	<p>Determines whether the use of Natural system commands is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether the use of Natural system commands is allowed:</p> <ul style="list-style-type: none"> • If the access level is CONTROL or higher, the use of system commands is allowed. • If the access level is lower than CONTROL, the use of system commands is not allowed. <p>If this option is set to "Y", the Natural profile parameter NC as well as any settings concerning system commands in Natural Security library profiles (Allow System Commands, Command Restrictions and Editing Restrictions) will be ignored.</p>
Set FUSER Read-Only	<p>Determines whether read-only access to the FUSER system file is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether modifications of the data on the FUSER system file are allowed:</p> <ul style="list-style-type: none"> • If the access level is ALTER, modifications on the FUSER file are allowed. This requires the definition of a Natural scratch-pad file (as described in the Natural Operations documentation for mainframes). • If the access level is lower than ALTER, modifications on the FUSER file are not allowed. <p>If this option is set to "Y", the RO option of the Natural profile parameter FUSER is ignored.</p>

RPC Options

Option	Explanation
Protect Services	<p>Determines if the Natural RPC service access is to be checked via the SAF server (Y/N).</p> <p>If you specify "N", only the service access is checked.</p> <p>If you specify "Y", the service access and the Natural Security library profile are checked.</p>
with Environment	<p>Determines whether the environment alias is to be used for the service-access check (Y/N).</p> <p>See also Definition of System-File Environments below.</p>

User-Resource Options

Option	Explanation
Allow Undef. Resources	Determines whether access to undefined resources is to be allowed via the Natural SAF Security user exits (Y/N). This option is only relevant if RACF is used as the external security system. With other external security systems, this option will be ignored.
with Environment	Determines whether the environment alias is to be used as prefix to the resource definitions (Y/N). See also Definition of System-File Environments below.

Definition of System-File Environments

This function is used to define environment profiles, that is, security profiles for the individual system-file combinations.

If you wish to protect resources in specific environments, you have to define environment profiles for these environments. In an environment profile, you specify a one-character alias for the environment. The alias is used identify the environment to the external security system; the environment-specific resource profiles whose names are prefixed with this alias determine users' access rights, if the "with Environment" option for the resource class in question is set to "Y" in the General NSF Options (see above).

For any environment-profile modifications to take effect, you have to restart your Natural session.

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 2, select "Definition of System-File Environments". The Define System-File Environments screen will be invoked.

Define System-File Environments Screen

The Define System-File Environments screen displays a list of all environment profiles which have been defined.

For each environment profile, its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT), name, alias (AL) and protection status (P) are displayed. The protection status can be:

I	The environment profile is inactive (both NSC and NSF Protection = N in the environment profile) .
N	The environment is only evaluated by Natural Security (NSC Protection = Y in the environment profile).
S	The environment is only evaluated by the SAF server (NSF Protection = Y in the environment profile).

Available Functions

The following functions are available:

Code	Function
AD	Add new environment profile. (You can also invoke this function by entering "AD" in the Command line.)
MO	Modify environment profile.
DE	Delete environment profile.
DI	Display environment profile.

To invoke a function for an environment, you mark the environment with the appropriate function code in column "Co".

Components of an Environment Profile

When you add a new environment or modify an existing one, the Define Environment Profile screen will be displayed. The items you can define as part of an environment profile on this screen and any subsequent screens/windows are:

Field	Explanation
Environment Name	You can specify a descriptive name for the environment profile.
Alias	<p>You specify a one-character alias for the environment profile. This alias is used in the external security system to define the resources related to the system-file combination of this environment.</p> <p>It is possible for multiple environment profiles to share the same alias. The rules defined for an alias in the external security system apply to all system-file combinations in whose environment profiles this alias is specified.</p>
General Options	<p>You specify the protection status of the environment:</p> <p>NSF Protection - If set to "Y", this activates the environment for validation by the SAF server - provided that the option "Protect Environment" in the General NSF Options (see above) is set to "Y".</p> <p>NSC Protection - If set to "Y", this activates the environment for validation by Natural Security.</p> <p>If both are set to "N", the environment is not evaluated. It is not possible to set both to "Y".</p>
System Files	<p>You define the environment by specifying the database IDs and file number of each system file (FUSER, FDIC, FSEC, FNAT). This combination of system files identifies the environment and must be unique.</p> <p>Once entered, the values of these fields cannot be changed.</p>

Additional Options

If you either mark the field "Additional Options" with "Y" or press PF4, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

They correspond to the options of the same names in Natural Security library profiles, as described in the Natural Security documentation.

NSF Online Services

Before you can use NSF Online Services, you have to define a utility security profile for the utility SYSNSFOS (which contains the NSF Online Services) in Natural Security.

NSF Online Services provides several functions for monitoring the SAF server.

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 2, select "NSF Online Services".

The Online Services menu will be displayed. It provides the following functions:

- System Parameters
- System Statistics
- User Statistics
- Zap Maintenance
- Storage Display
- System Tracing
- Server Restart

System Parameters

This function display the parameter settings as defined in the system parameter module. The following information is displayed:

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server that are related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Class/Type	Shows the names of the different SAF general resources Classes or Types. These contain either the default or any override values which have been defined in the system parameter module.
Universal	This indicates a particular check is designated universal. If selected, then failure to define a particular resource profile will result in all users having access to it. Natural Program execution authorization cannot be designated universal.
Buffered	Displays for each type of check the maximum number of positive checks that the SAF server can buffer on behalf of each user.
Logging	This indicates the SMF logging level required when performing security checks. "0" signifies logging ASIS, that is, in accordance with the default for the security Class/Type; "1" indicates an override setting of NONE.
Active	Designates the particular authorization checks that are active. This applies only to checks performed by mainframe Natural as all other checks are activated by the installation process.
Env (Environment)	Indicates that an environment code, based on the Natural system files, is used to prefix certain resource profiles. Applies only to authorization checks performed by mainframe Natural.

Storage (k)	The size of the buffer in kilobytes which can be used for caching positive security checks in the address space of the SAF server.
Server DBID	Shows the database ID used by the SAF server.
Encrypt Req.	Indicates whether security requests passed between different SAF server components are communicated encrypted.
Encrypt Stg.	Indicates whether storage maintained within the Natural environment is kept in an encrypted state.
Messages	SAF server message level: Level "0" gives only error message, "1" reports security violations and "3" generates an audit trail of all checks.
Cmd Log	Indicates whether command logging is turned on.
Buffer	Indicates whether security checks will be cached by the SAF server.
JCL check	Indicates whether CA-JCL check processing is available within the Natural environment.
Prefix Prog	Indicates whether Natural program names are prefixed with the name of the current application library when performing authorization checks. <i>Not applicable to Natural SAF Security.</i>
Protect Obj	Indicates whether program objects are protected within the Natural environment. Users require ALTER access to a particular application in order to modify its program objects. <i>Not applicable to Natural SAF Security.</i>
Log SYSMAIN	Indicates whether logging of all SYSMAIN operation is required. <i>Not applicable to Natural SAF Security.</i>
SYSMAIN/Lib	Indicates whether authorization checks for SYSMAIN functions will include access to the relevant Natural application libraries. <i>Not applicable to Natural SAF Security.</i>
Cmd Line	Indicates whether the Natural command line is protected. Users require CONTROL access in order to enter commands in the Natural command line.
ETID	Indicates whether Natural will generate a unique ETID.
Edit/Lib	Indicates whether Natural will prevent editing of objects located in another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Clear/Ed	Indicates whether Natural will clear the edit area when logging onto another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Ext Name	Indicates whether Natural will take the user name from SAF. Specifically, the field *USER-NAME will be taken from RACF or CA-ACF2.
Ext Group	Indicates whether Natural will take the group name from SAF. That is, the field *GROUP will be taken from RACF, CA Top Secret, CA-ACF2.
Log API	Indicates whether SMF logging is performed when executing the Natural API.
Env API	Indicates whether authorization checks performed by the Natural API will be prefixed by an environment code based on the Natural system files.

System Statistics

This function displays statistical information on the SAF server. The following information is displayed:

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Check (+ve)	Indicates the number of authorization checks performed against the security system for each check type. The count indicates authorizations for which access was permitted and can include universal checks.
Check (-ve)	Indicates the number of authorization checks performed against the security system for which access was denied.
Check saved	Shows the number of authorization checks that were optimized by the SAF server because the result was already known.
Overwritten	Number of times positive authorization results were overwritten in the SAF server's cache because more recent information took its place in the buffer. Increase the number of items buffered if this count is excessive for any particular check type.
Lngh	Number of bytes reserved to cache resource profiles belonging to each type of authorization check. This value is generated automatically by the system.
Active Users	Number of users currently active in the SAF server.
High Watermark	High watermark value for number of users present in the SAF server.
Max Users	Maximum of users that can be accommodated.
Overwritten	Number of times a user area was reclaimed and allocated to another user. Increase the total buffer size if this count becomes excessive.
Authenticated	The total number of successful authentication checks performed.
Denied	The number of unsuccessful authentication checks.

User Statistics

This function displays statistical information on the currently active users. The function displays a list of users. When you select a user from the list, statistical information on this user will be displayed. The individual items correspond to the items of the same names as described above for System Statistics.

Zap Maintenance

This function displays a list ZAPs applied to the SAF server.

Storage Display

This function displays the storage of the SAF server's address space.

System Tracing

This function displays a list of the 256 most recent trace events.

Server Restart

This function is used to restart the SAF server. The Restart function ensures that all data held in the SAF server's own buffer are flushed. In addition, any data held by the security system itself in the address space of the SAF server are flushed by this action.

User Exits

This section describes the user exits provided by Natural SAF Security. It covers the following topics:

- Overview of User Exits
- User Exits for User and Password Authentication
- User Exit for Checking Resource Access to Dedicated API Class
- User Exit for Maintaining Resource Profiles
- User Exit for Checking Access Rights to a Resource
- User Exit for Obtaining Information from the SAF Server

Overview of User Exits

Natural SAF Security provides the following user exits:

Function	Invoked Subprogram	Example Program of how to Invoke the Subprogram
User and password authentication.	NSFNPAS	PGMSFU01
	NSFNPASZ	PGMSFU02
	NSFNPAX	PGMSFU03
Check resource access to a dedicated API class.	NSFNAPC	PGMSFC nn
Maintain resource profiles.	NSFNRES	PGMSFR nn
Check access rights to a resource.	NSFNRES	PGMSFX nn
Obtain miscellaneous information from the SAF server.	NSFNINF	PGMSFI nn

The example programs are provided in the Natural Security library SYSSEC.

User Exits for User and Password Authentication

- NSFNPAS
- NSFNPASZ
- NSFNPAX

NSFNPAS

The subprogram NSFNPAS can be called from any Natural library to verify the authentication of a user (*USER) and, optionally, establish that the user was already logged on.

Five different sub-call are available:

#PAS-FUNC	Action
INDQVER	Verify user ID (not password) and create ACEE.
INDQVPW	Verify user ID and password, creating new ACEE.
INDQVPO	Verify user ID and password without creating new ACEE (CA Top Secret only).
INDQVPT	Verify user ID and password without creating ACEE (CA Top Secret only).
INDQVPC	Verify user ID and password and change password creating new ACEE.

The parameter data area NSFAPAS is available to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#PAS-FUNC	B1	Indicates type of verification check required.
#PAS-RETC	B1	Return code: 8 = error; 16 = severe error.
#PAS-POLD	A8	Existing (old) password.
#PAS-PNEW	A8	New password.
#PAS-ACCN	A8	Accounting information - <i>for future use</i> .
#PAS-SERR	B8	Return code (as described in the SAF Security Kernel documentation).

NSFNPASZ

To verify the password of any other user ID, the subprogram NSFNPASZ is provided.

The parameters are the same as described for subprogram NSFNPAS above.

In addition, the parameter data area NSFAPAS contains the following fields for NSFNPASZ:

Field	Format/Length	Description
#PAS-PUSER	A8	User ID of user whose password is to be changed.
#PAS-PMSG	A40	Message text returned from the SAF server.

NSFNPAX

To verify and change the password of *USER, the subprogram NSFNPAX is provided.

The parameters are the same as described for subprogram NSFNPAS above.

In addition, the parameter data area NSFAPAS contains the following fields for NSFNPAX:

Field	Format/Length	Description
#PAS-PUSER	A8	<i>Not used.</i>
#PAS-PMSG	A40	Message text returned from the SAF server.

User Exit for Checking Resource Access to Dedicated API Class

The subprogram NSFNA PC can be called from any Natural library to check the access to a general resource profile.

Input Parameters:

Parameter	Content
#RES-PROF	Name of desired profile.
#RES-CLAS	Name of desired class.
#RES-ATTR	Access level to be checked: H'02' = READ access, H'04' = UPDATE access; H'08' = CTL access, H'80' = ALTER access. If you specify H'00', the highest access level will be returned.

Output Parameters:

Parameter	Content
#RES-ATTR	If H'00' was specified as input, this field returns the highest acceptable access level.
#RES-RETC	Return code: 0 = Profile allowed for given access level. 8 = Error (in this case, the field #RES-SERR contains the SAF error code).

User Exit for Maintaining Resource Profiles

The subprogram NSFNR ES can be called from any Natural library to read and maintain security-profile information.

RACF, CA Top Secret and CA-ACF2 enable different levels of functionality to be achieved. The different functions are shown below:

#RES-FUNC	Action
INDQRTV	Retrieve field(s) from user, group, and general profiles of the security system. CA Top Secret and CA-ACF2 allow fields such as PGMRNAME to be read from a base segment.
INDQRDN	Retrieve next resource profile in collating sequence. The name of the resource and selected field(s) can be retrieved. CA Top Secret permits only the USER class to be retrieved in this way. This functionality is currently not available with CA-ACF2.

The parameter data area NSFARES available to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#RES-FUNC	B1	Indicates function type required.
#RES-ATTR	B1	<i>Not used for this call.</i>
#RES-RETC	B1	Return code: 0 = call successful ; 4 = profile not found/EOL; 8 = error.
#RES-CLAS	A8	Required resource class/type.
#RES-GRUP	A8	Default user group - returned.
#RES-PROF	A32	Name of resource profile.
#RES-FLDA	A8 * 4	Profile field names (array).
#RES-SERR	B8	8-byte return code (as described in the SAF Security Kernel documentation).
#RES-SLOG	A4	<i>Reserved for future use.</i>
#RES-DATA	A16 * 16	Profile data input/output area. The data layout is described in detail in IBM RACROUTE documentation.

User Exits for Checking Access Rights to a Resource

The subprogram NSFNRRES can be called from any Natural library to test a user's authorization to any resource profile, including those used to protect Natural objects.

#RES-FUNC	Action
INDQCHK (#RES-ATTR supplied)	Check authorization at given level of access.
INDQCHK (#RES-ATTR zero)	Determine user's maximum access level.

The parameter data area NSFARES is provided to invoke this subprogram. Its fields are:

Field	Format/Length	Description
#RES-FUNC	B1	Indicates function type required
#RES-ATTR	B1	Access level to be tested; either zero or determine highest level (as described in the IBM RACROUTE documentation).
#RES-RETC	B1	Return code: 0 = success; 8 = error.
#RES-CLAS	A8	Resource class/type.
#RES-PROF	A32	Name of resource profile.
#RES-SERR	B8	8-byte return code (as described in SAF Security Kernel documentation).

User Exit for Obtaining Information from the SAF Server

The subprogram NSFNRINF is provided to perform a number of functions which may be useful when using Natural SAF Security.

The different functions provided are:

#INFFUNC	Action
INF-1	Determine last "access denied" message for this user.
INF-2	Determine last "access denied" message - internal format.
INF-3	Return invocation count.
INF-4	Return environment code.
INF-5	Read user name and group from values stored.
INF-6	Update user-name/group values; for example, if these are to be reformatted.
INF-7	<i>Currently not available.</i>
INF-8	<i>Currently not available.</i>
INF-9	Write SMF record.

The parameter data area NSFAINF is provided to invoke this subprogram. The local data area NSFLEQU defines the necessary equate values.

Field	Format/Length	Description
#INFFUNC	B2	Indicates function type required.
#INFRETC	I2	Return code: zero = success.
#INFDATA-SUBR	I4	Error - sub-response.
#INFDATA-TEXT	A72	Last error message.
#INF-COUNT	I4	Invocation count.
#INF-ENV	A1	Current environment code.
#INF-GROUP	A8	Group.
#INF-NAME	A32	User name.
#INF-SMFLLEN	B1	Length of SMF data to be written.
#INF-SMFTXT	B255	Data to be written - A15 * 17.